

Kwantlen Polytechnic University Research Data Management Strategy – v1.3

Table of Contents

- Preamble 1
 - Background 1
 - Key Definitions 2
 - Why Research Data Management? 3
 - Scope 3
 - Oversight and Review 4
- Strategic Priorities 4
 - 1. Institutional policy and governance** 4
 - 2. Awareness and education** 5
 - 3. Support for Researchers** 5
 - 4. Context-based approach** 6
- Contact 6
- Appendix A: Relevant Policies and Legislation 7
- Appendix B: Glossary 7

Preamble

Background

Research is a time-honoured example of KPU’s motto, “where thought meets action”. In the Vision 2023 Strategic Plan, KPU announced its intention to increase the levels of activity, funding, and intensity of research and scholarship, and Goal 3 of the complementary Academic Plan 2023 also focuses on the acceleration of research at KPU. This commitment to growing KPU’s research capacity comes with an accompanying responsibility to ensure that research practices are evolving to meet the standards of the modern scholarly ecosystem. One area of significant paradigm shift involves new expectations around the management and accessibility of research data.

In March 2021, the joint federal granting agencies of Canada - the [Canadian Institutes of Health Research \(CIHR\)](#), the [Natural Sciences and Engineering Research Council of Canada \(NSERC\)](#), and the [Social Sciences and Humanities Research Council of Canada \(SSHRC\)](#), collectively called the Tri-Agencies - passed the [Tri-Agency Research Data Management Policy](#). The policy outlines the phased introduction of

new research data management (RDM) requirements affecting both institutions that administer Tri-Agency funding, and researchers receiving that funding.

The first element of the policy requires that “each postsecondary institution [...] eligible to administer CIHR, NSERC or SSHRC funds is required to create an institutional RDM strategy and notify the agencies when it has been completed.” The other two elements establish requirements for researchers to submit Data Management Plans (DMPs) and/or deposit their data in a data repository as a condition of certain funding opportunities.

The KPU Research Data Management Strategy (hereafter referred to as “the Strategy”) not only fulfills KPU’s obligation to the Tri-Agencies, it represents a broader institutional commitment to the adoption and promotion of good RDM practices as an important component of research excellence. By building RDM capacity, the university supports its researchers in meeting their own emerging RDM responsibilities.

Key Definitions

Research data

Data that are used as primary sources to support technical or scientific enquiry, research, scholarship, or creative practice, and that are used as evidence in the research process and/or are commonly accepted in the research community as necessary to validate research findings and results. Research data may be experimental data, observational data, operational data, third party data, public sector data, monitoring data, processed data, or repurposed data. What is considered relevant research data is often highly contextual, and determining what counts as such should be guided by disciplinary norms.” (Tri-Agency Research Data Management Policy, “[Frequently Asked Questions](#)”, Government of Canada 2021)

Research data management (RDM)

Data Management refers to the storage, access and preservation of data produced from a given investigation. Data management practices cover the entire lifecycle of the data, from planning the investigation to conducting it, and from backing up data as it is created and used to long term preservation of data deliverables after the research investigation has concluded. Specific activities and issues that fall within the category of data management include: file naming; data quality control and quality assurance; data access; data documentation; metadata creation and controlled vocabularies; data storage; data archiving and preservation; data sharing and reuse; data integrity; data security; data privacy; data rights; notebook protocols. (Research Data Management Terminology, “[Research Data Management](#)”, CODATA 2021)

Sensitive Data

Information which must be protected against unauthorized access or disclosure due to its potential to cause harm to a person, organization, or entity. This includes personally identifiable information (such as name, ID numbers, education, health, genetic, financial, criminal, or location data; see [What is Personal Information](#) under the federal *Privacy Act*), confidential business information (such as trade secrets or intellectual property), and other forms of data that are provided in confidence (such as classified government information). Data sensitivity exists on a spectrum, with varying levels of risk and impact depending on the context of its

creation, use, and disclosure. Many kinds of data may become sensitive under certain conditions or in combination with other data.

Why Research Data Management?

In recent years, the concept of research data as a first-class output of research has gained considerable traction worldwide. As a corollary of this, the scholarly community is increasingly recognizing the importance of good data management to preserve these valuable outputs. Benefits of RDM include:

- improved transparency, accountability, and reproducibility of the research process
- protection of the Confidentiality, Integrity, and Availability of valuable research data to mitigate risk of loss, theft, or corruption
- acceleration of new discoveries through data sharing and reuse
- enhanced efficiency and ease in research workflows and collaboration throughout the entire research lifecycle

Funding agencies and scholarly publishers now also regularly suggest or require data management practices such as Data Availability Statements, data sharing, Data Management Plans (DMPs), and data deposit in repositories as a condition of funding or publication.

KPU acknowledges the value of research data as an important research output, and commits to supporting its faculty, staff, students, and partners in establishing good RDM protocols aligned with internationally accepted best practices and standards. Where such support does not yet exist, KPU recognizes the need to fill these gaps by developing or providing access to tools, services, infrastructure, and resources.

Government and community frameworks informing KPU's RDM Strategy include the [TCPS-2, Tri-Agency Statement of Principles on Digital Data Management](#), [FAIR Guiding Principles for scientific data management and stewardship](#), [CARE Principles of Indigenous Data Governance](#), and the [First Nations Principles of OCAP](#)[®]. Indigenous ethical criteria as outlined in the [United Nations Declaration on the Rights of Indigenous Peoples](#) (UNDRIP) take precedence in matters related to Indigenous data. When working in Canada a [distinctions-based approach](#) to research with First Nations, Métis, and Inuit peoples of Canada is recommended by the [Declaration on Rights of Indigenous Peoples Act](#) (DRIPA).

Scope

The KPU RDM Strategy is a high-level guiding document designed to establish the university's priority areas for the development of RDM support over the next 2 to 3 years, from 2023 through 2025 or until a new KPU Strategic Plan is launched. Recommendations made by, and in response to, the Strategy apply to all research conducted under the auspices of the university, not only research funded by the Tri-Agencies; it represents an institution-wide effort to initiate a coordinated and cohesive approach to RDM at KPU.

The Strategy is not a policy detailing specific requirements and responsibilities, nor is it an implementation plan; putting its strategic priorities into action will require dedicated ongoing time, effort, and resources. The Strategy also does not represent an open data mandate. While KPU endorses the movement towards openness in science, government, and education, the degree to which data can and should be made open is dictated by complex contextual factors such as ethics, privacy, legal, and

cultural considerations. In this, the university will follow the approach of making data “as open as possible, as closed as necessary.”

Oversight and Review

The Strategy was initially drafted by the RDM Strategy Librarian under the supervision of the University Librarian and AVP Research and the guidance of the Institutional RDM Strategy Working Group, consisting of representatives from the Library, Office of Research Services, Research Ethics Board, IT, Information Security, Privacy Office, Teaching and Learning Commons, and faculty and staff researchers. Feedback was also solicited from the Senate Standing Committee on Research and Graduate Studies, the senior executive, faculty Research and Scholarship Committees, and the broader KPU community during a 3-week public consultation period in January 2023.

The Strategy will need to be periodically revisited and adapted as RDM services are established and best practices in the field evolve. To perform this necessary upkeep, an RDM implementation committee shall be formed in early Spring 2023, subsequent to publication of the first version of the Strategy, to collaborate on an action plan that sets concrete goals and timelines. The committee will meet regularly to review implementation efforts and update the Strategy.

Strategic Priorities

1. Institutional policy and governance

a. Responsibility

Define clear and centralized responsibility for RDM within KPU.

- i. Establish an RDM Strategy implementation committee with members from a cross-section of stakeholder units to develop an action plan, review efforts to implement the Strategy’s priorities, and update the Strategy on an ongoing basis.

b. Clarity

Identify, make explicit, and/or create policies that address research data, and ensure the implications of these policies are widely understood within the research community.

- i. Perform a full review of institutional policies that affect research data in order to determine if amendments or additions are needed.

c. Consistency

Align new RDM practices and information resources with existing and future KPU policy and priorities.

- i. Determine and secure necessary resources to provide RDM support for the increased research activity, funding, and impact of research mandated by goal C2 of the Vision 2023 Strategic Plan.
- ii. Revisit the Strategy and RDM priorities and service offerings in response to the new Strategic and Academic Plans to be developed in the near future.

2. Awareness and education

Overall awareness of RDM and its value to different constituents needs to be significantly improved not only within KPU but nationwide. A key component of the implementation and utilization of RDM is the provision of training and education both to researchers (faculty, staff, students, partners) and to institutional staff who will provide support for data management services (librarians, ORS, IT).

a. Train

Invest in staff training and hiring for RDM expertise to increase support capacity.

b. Network

Identify and build relationships with key 'data champions' within the research community to promote a culture of increased RDM knowledge and practice.

c. Leverage

Capitalize on existing institutional groups and platforms to provide information and guidance on RDM best practices.

d. Consolidate

Establish a central KPU RDM resource hub to coordinate cross-unit RDM support efforts.

e. Participate

Get involved in national and international RDM initiatives, working groups, and communities to stay current with, and contribute to, the development of standards and practices.

3. Support for Researchers

To support the Academic Plan Goal of accelerating research at KPU, it is critical that the university provide access to the information and tools its faculty, staff, and student researchers need to navigate RDM requirements laid out by funders, publishers, ethics boards, and information security compliance standards. Allocating resources to ease the administrative burden of these new responsibilities on researchers demonstrates institutional commitment and encourages adoption of RDM practices, helping the community grow to appreciate the benefits to their own work.

a. Investigate

Engage in dialogue with the research community to determine needed supports for all disciplines and types of research being conducted at KPU, including applied, course-based, student-conducted, Scholarship of Teaching and Learning, etc.

b. Create and Iterate

Launch pilot projects aimed at providing KPU researchers with resources and services to help them meet internal and external requirements, including but not limited to:

- i. *Data Management Plans (DMPs)*: Provide tools and guidance for completing DMPs, such as templates and harmonization with REB applications
- ii. *Data storage*: Facilitate access to storage options at all stages of the research lifecycle, over the short (active research), medium (dissemination), and long term (preservation or disposal).

- iii. *Sensitive data*: Clarify responsibilities and solutions to comply with information security, privacy, and confidentiality needs where unauthorized access to data may result in harm to individuals or organizations.
 - iv. *FAIR data and metadata*: Where appropriate, assist researchers in enhancing data findability, accessibility, interoperability, and reusability for sharing and secondary use.
- c. **Collaborate**
Seek out opportunities to work with other institutions to pool RDM resources and take advantage of community expertise, tools, and shared services.
 - d. **Celebrate**
Showcase exemplars of RDM adoption and its benefits within the KPU community.

4. Context-based approach

As a Polytechnic Special Purpose Teaching University, KPU's research profile is unique, and care must be taken to ensure any services developed address responsibilities and considerations relevant to our diverse researchers, partners, and communities.

- a. **Students**
As a teaching-focused postsecondary institution, ensure current RDM best practices are included in the education, training, and mentorship of student researchers.
- b. **Community**
Tailor RDM at the project level to the unique considerations for research and outreach initiatives within the regions KPU serves. Build public trust through responsible, transparent data stewardship practices.
- c. **Applied research**
Work with our industry, government, and nonprofit research partners to implement RDM protocols compatible with applicable legal requirements and contractual obligations.
- d. **Indigenous data sovereignty**
Where research involves Indigenous data, establish partnerships and work closely with the relevant Indigenous communities and advisory groups to ensure research data is managed in accordance with those communities' rights and preferences, and well as with [UNDRIP](#) and the [CARE Principles of Indigenous Data Governance](#). In Canada specifically, [DRIPA](#) and the [First Nations Principles of OCAP®](#) apply for research involving First Nations, Inuit, or Métis to support respectful research with these communities.

Contact

Questions, comments, and feedback about the Institutional Strategy should be directed to rdm@kpu.ca.

Appendix A: Relevant Policies and Legislation

- Internal
 - [VISION 2023 Strategic Plan](#) – Section C: Creativity
 - [Academic Plan 2023 - Research](#)
 - IM1 [Copyright Compliance / Procedure](#)
 - IM2 [Freedom of Information / Procedure](#)
 - IM3 [Information and Educational Technology Usage / Procedure](#)
 - IM4 [Confidentiality / Procedure](#)
 - IM7 [Management of Surveys / Procedure](#)
 - IM8 [Privacy / Procedure](#)
 - IM9 [Information Security / Procedure](#)
 - RS1 [Research Involving Human Participants / Procedure](#)
 - RS2 [Integrity in Research and Scholarship / Procedure](#)
 - RS3 [Indirect Costs of Research / Procedure](#)
 - RS4 [Administration and Control of Research and Special Funds / Procedure](#)
 - RS5 [Intellectual Property / Procedure](#)
 - [KPU-KFA Collective Agreement](#)
- External
 - [Tri-Agency Framework: Responsible Conduct of Research \(2021\)](#)
 - [Tri-Agency Research Data Management Policy \(2021\)](#)
 - [Tri-Agency Statement of Principles on Digital Data Management](#)
 - [Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 \(2018\)](#)

Appendix B: Glossary

Applied research: Original investigation undertaken in order to acquire new knowledge. It is, however, directed primarily towards a specific, practical aim or objective. (OECD. (2015). “Glossary of terms”, in Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, OECD Publishing, Paris. <http://dx.doi.org/10.1787/9789264239012-17-en>)

Availability: Assurance that the systems responsible for delivering, storing and processing information, and the information itself, are accessible and usable when needed, by those who need them, to support business functions. A goal of information security is to ensure availability. (Government of British Columbia. “Availability.” *Information Security Glossary*. <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/information-security-glossary>. Accessed 8 Dec. 2022.)

Confidentiality: Assurance that information is shared only among authorised persons or organisations. Breaches of confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc. The classification of the information should determine its confidentiality and hence the appropriate safeguards. (Government of British Columbia. “Confidentiality.” *Information Security Glossary*. <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/information-security-glossary>. Accessed 8 Dec. 2022.)

[for-government/information-management-technology/information-security/information-security-awareness/information-security-glossary](https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/information-security-glossary). Accessed 8 Dec. 2022.)

Data Management Plan: A formal statement describing how research data will be managed and documented throughout a research project. Most DMPs contain the following core elements: metadata; policies for data access, sharing, re-use and redistribution; and plans for archiving preservation and destruction. (Sensitive Data Expert Group. (2020). *Sensitive Data Toolkit for Researchers Part 1: Glossary of Terms for Sensitive Data used for Research Purposes*. Zenodo. <https://doi.org/10.5281/zenodo.4088946>)

Data Repository: A place where researchers can submit their data to be stored and managed. Data repositories may have specific requirements regarding subject, research domain, format or data re-use. Others are open to receiving a broad variety of data. Materials in data repositories are ideally curated and stewarded to ensure they are authentic, discoverable, and appropriately accessible over the medium term. (Sensitive Data Expert Group. (2020). *Sensitive Data Toolkit for Researchers Part 1: Glossary of Terms for Sensitive Data used for Research Purposes*. Zenodo. <https://doi.org/10.5281/zenodo.4088946>)

Integrity: The characteristic of information being authentic, accurate and complete and the preservation of accuracy and completeness by protecting the information from unauthorized, unanticipated, or unintentional modification. The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon. (Government of British Columbia. "Integrity." *Information Security Glossary*. <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/information-security-glossary>. Accessed 8 Dec. 2022.)